

Digital Forensics Lab Guidelines

(Part 1)

Aung Zaw Myo (ThirdEye)

12/10/2019

Keep Mind Pure...!! BE Good To Other..!!

Digital Forensics သည် Forensics Science ရဲ့ အခွဲတစ်ခုဖြစ်ပြီး Digital Device, Digital Storage များကို ခွဲခြမ်းစိတ်ဖြာခြင်း၊ လည်းကောင်း Device များ Storage များကို မူရင်းအတိုင်းကူးယူခြင်း၊ စစ်ဆေးခြင်း ၊ တွေ့ရှိချက်များကိုတရားရုံးတွင် တင်ပြခြင်း အပိုင်းတို့ပါဝင်ပါသည်။ ရှာဖွေစစ်ဆေးတွေ့ ရှိချက်များ ကိုတော့ Electronic Evidence သို့မဟုတ် Digital Evidence လို့သတ်မှတ် ခေါ်ဆိုပါတယ်။ စစ်ဆေးတွေ့ရှိချက်တွေဟာ တရားရုံးမှာ လက်ခံနိုင်တဲ့ Evidence တွေ အချက်အလက်တွေဖြစ်ရပါမယ်။ အခုအများကခေါ်ဆိုနေတဲ့ Cyber Crime ပြစ်မှုတွေ ဟာ မိမိနိုင်ငံတစ်ခုရဲ့ နယ်နိမိတ်ထဲမှာတင်မက Borderless ဖြစ်နိုင်တာကြောင့် စုံစမ်းစစ်ဆေးပြီးမှ ရရှိလာတဲ့သက်သေခံအချက်အလက်တွေဟာ မိမိနိုင်ငံမှ တရားရုံးက လက်ခံနိုင်တဲ့ Evidences တွေဖြစ်ရုံသာမက နိုင်ငံတစ်ကာမှ လက်ခံ နိုင်တဲ့ Evidence မျိုးဖြစ်ရပါမယ်။ google ကနေ အချက်အလက်ဘယ်လို တောင်းခံလို့ ရနိုင်တယ်ဆိုတာဖော်ပြပြီးပါပြီ။ (ယနေ့အထိတော့ တောင်းခံထားတဲ့ အချက်အလက် မတွေ့ရသေးပါ။) facebook ကနေတော့ ယနေ့အချိန်အထိ ၄ ကြိမ်ခန့်သာတောင်း ဆိုထားတာတွေ့ရပါတယ်။ Digital Evidence, Electronic Evidenceတွေက အခြား လက်ဗွေ DNAတို့နဲ့မတူပါဘူး

- သက်သေခံအချက်အလက်တွေဟာ နေရာတစ်နေရာထဲတင်မက အခြား နေရာများတွင်ပါရှိနိုင်ပါတယ်။
- သက်သေခံအချက်အလက်တွေဟာ အချိန်အခါမရွေး စက္ကန့်ပိုင်းအတွင်း ပြောင်းလဲနိုင်ပါတယ်။
- သက်သေခံအချက်အလက်တွေကို ခနလေးနဲ့ ဖျက်ဆီးနိုင် ပြောင်းလဲနိုင်ပါ တယ်။
- သိမ်ဆည်းမိတဲ့ Electronic Device တွေက အခြားသက်သေခံ ပစ္စည်း တွေလို နှစ်ကြာရှည်စွာထိမ်းသိမ်းထားဖို့ခက်ခဲနိုင်ပါတယ်။
- Digital Evidence, Electronic Evidence ကိုရယူတဲ့နေရာမှာ ပြဋ္ဌာန်းထားတဲ့ တရားဥပဒေ အရ တရားနည်းလမ်းကျစွာ ရယူရမှာဖြစ်ပါတယ်။
- Electronic Device တွေကို သိမ်းဆည်းမည့်သူနှင့်စစ်ဆေးမည့်သူတွေကို လိုက်နာရမည့်အချက်တွေ ၊ သိမ်းဆည်းပုံကိုယ်တွယ်ထိမ်းသိမ်းပုံ၊ စစ်ဆေးပုံ တို့အတွက် လိုအပ်တဲ့ သင်တန်းတွေပေးထားရပါမယ်။
- သိမ်ဆည်းသူ၊စစ်ဆေးသူတွေက မည်သည့်နည်းနှင့်မှ Electronic Device ထဲမှာပါတဲ့ အချက်အလက်တွေကို ပြင်ဆင်ပြောင်းလဲခြင်းမပြုရပါ။ အတွင်းပိုင်း အချက်အလက်ကို

ရယူရန် ဒါမှမဟုတ် System Setting ကိုပြောင်းလဲဖို့ လိုအပ် လာလျှင် ဥပဒေအတိုင်းသာ ပြင်ဆင် ကိုယ်တွင် နိုင်ပါတယ်။

- ပြင်ဆင်တဲ့အရာ၊ အချက်အလက်တွေကိုရယူတဲ့အခါမှာ ဥပဒေအတိုင်း အသေးစိတ်ရယူပုံ လုပ်ဆောင်ပုံတွေကို မှတ်တမ်းတင်ထားရပါမယ်။ လိုအပ်ရင် သက်သေများရှေ့မှောက်မှာ ပြုလုပ်ရပါမည်။

- စစ်ဆေးသည့်နည်းလမ်းလုပ်ဆောင်ပုံအဆင့်ဆင့်ကိုမှတ်တမ်းတင်ထားရမည့်အပြင် လိုအပ်လာလျှင် သက်သေခံ အချက်အလက်များအား အခြား အဖွဲ့ အစည်းတစ်ခုမှ စစ်ဆေးတဲ့အခါမှာ ရရှိလာတဲ့ အဖြေက အတူတူပဲ ဖြစ်ရပါမည်။

Digital Forensics lab မစတင်မှီမှာ Research အနေနဲ့ပြုလုပ်ထားသင့်တဲ့ အကြောင်းအရာတွေရှိပါတယ်။ ယခင်နှစ်တွေအရ လက်ရှိအနေအထား အရဖမ်းဆီးသိမ်းဆည်းမိတဲ့ Electronic Device တွေကို ဘာတွေဖြစ်မလဲဘာတွေက အများဆုံးလဲ ဘယ်လိုမှုခင်းတွေလဲ ဘယ်နေရာတွေကနေ အများဆုံးသိမ်း ဆည်းမိလဲ ၊ စတင်သိမ်းဆည်းသူတွေက အရည်အချင်းပြည့်မှီရဲ့လား၊ ဘယ်လိုအားနည်းချက်တွေရှိလဲ အားသာချက်တွေရှိလဲ သိမ်းဆည်းမိတဲ့ Electronic Device တွေကနေ ဘယ်လောက်အတိုင်းအတာအထိ Digital Evidence, Electronic Evidence တွေရယူနိုင်ခဲ့သလဲ ၊ စစ်ဆေးတဲ့ လူတွေရဲ့ အားနည်းချက် အားသာချက်က ဘာရှိလဲ ဘာတွေထပ်လိုအပ်လဲ စတဲ့ အချက်တွေကို စနစ်တကျ Research လုပ်ရပါမယ်။ ရရှိလာတဲ့ Research တွေကနေ Digital Forensics lab မှာ လိုအပ်တာတွေကို ပြုပြင်ပြောင်းလဲခြင်း သို့မဟုတ် စတင်ဆောင်ရွက်ခြင်းများကို ပြုလုပ်ရပါမယ်။ ဒါတွေကို လေ့လာအကဲဖြတ်ပြီးမှသာ lab ပမာဏကို တွက်ချက်တည် ဆောက်ရပါမယ်။ နောက်ထပ်လိုအပ်တဲ့ အရေးကြီးတဲ့ အချက်ကတော့ နိုင်ငံမှာပြဋ္ဌာန်းထားတဲ့တည်ဆဲဥပဒေ နိုင်ငံတစ်ကာဥပဒေတွေကို ကျွမ်းကျင်ပိုင်နိုင်စွာ သိရှိခြင်းဖြစ်ပါတယ်။ သိခြားအဖွဲ့အနေနဲ့ဖွဲ့စည်းထားသင့်ပါတယ်။ အခြားနိုင်ငံတွေက Lab များနဲ့ နှိုင်းယှဉ်လေ့လာရပါမယ်။ Lab ကိုစတင်တာပဲဖြစ်ဖြစ်၊ ပြုပြင်ပြောင်းလဲတာပဲဖြစ်ဖြစ် အောက်မှာ ဖော်ပြထားတဲ့ အချက်အလက်တွေကို လေ့လာထားသင့်ပါသည်။

- လွန်ခဲ့တဲ့ နှစ်တွေအလိုက် မှုခင်းတွေမှာ Electronic Evidence များကို အသုံးပြုပြီး အမှုဘယ်လောက်များများဖြေရှင်းနိုင်ခဲ့သလဲ

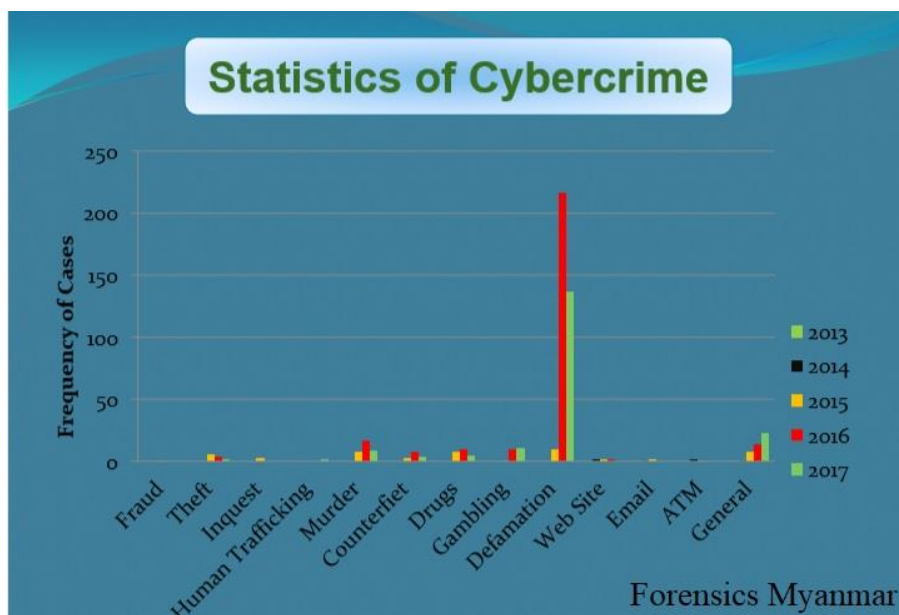
- ဘယ်လိုမှုခင်းတွေမှာ Electronic Evidence ကို အများဆုံး အသုံးပြုနိုင်ခဲ့သလဲ

- Digital Forensics ပြုလုပ်ရာမှာ ဘယ်သူတွေက ဘယ်လို Electronic Evidence

တွေကို စစ်ဆေးနိုင်ခဲ့သလဲဘယ်လိုနည်းပညာ နည်းလမ်းတွေကို အသုံးပြုနိုင်ခဲ့သလဲ

- ရလဒ်တွေက ဘယ်လိုလဲ အမှုတစ်ခုချင်းစီအလိုက် ပျမ်းမျှ ဘယ်လောက်ကုန်ကျသလဲ
- အပေါ်က အချက်တွေအရ ဘယ်လိုအရာတွေမှာ အားနည်းနေသလဲ အားသာနေသလဲ နောက်ထပ်ဘာတွေ လိုအပ်သလဲ
- မိမိတို့ Lab က အားနည်းချက်တွေက အခြား Lab တွေမှာရော ရှိသလား
- အခြား lab တွေက ပြင်ဆင်ပြီးခဲ့ရင် ပူးပေါင်းဆောင်ရွက်ရပါမည်။
- နောက်ထပ်တွက်ချက်ရမှာကတော့ အဆောက်အဦးစရိတ်၊ ပြင်ဆင်စရိတ်၊ Lab အတွက် လိုအပ်တဲ့ Hardware Software licence ကုန်ကျစရိတ် အမှုထမ်းလစာ သင်တန်းအလိုက်ကုန်ကျစရိတ် Hardware Software update နဲ့ maintenance နဲ့ replacement လုပ်တဲ့စရိတ်တို့ဖြစ်ပါတယ်။

Photo Source India Police and ASPCERT.



Myanmar Cyber Crime Statistics 2013-2017

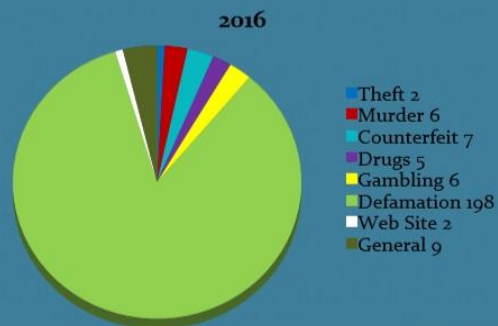
Statistics of Cybercrime Cases

In 2013	-	2 Cases
In 2014	-	6 Cases
In 2015	-	53 Cases
In 2016	-	281 Cases
In 2017	-	193 Cases
Total		535 Cases

forensics myanmar

Myanmar Cyber Crime Statistics 2013-2017

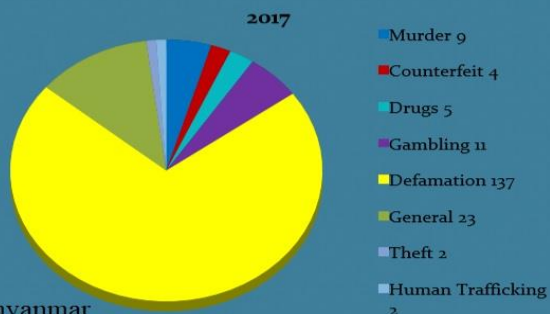
Cyber Crime Cases in Myanmar 2016



forensicsmyanmar

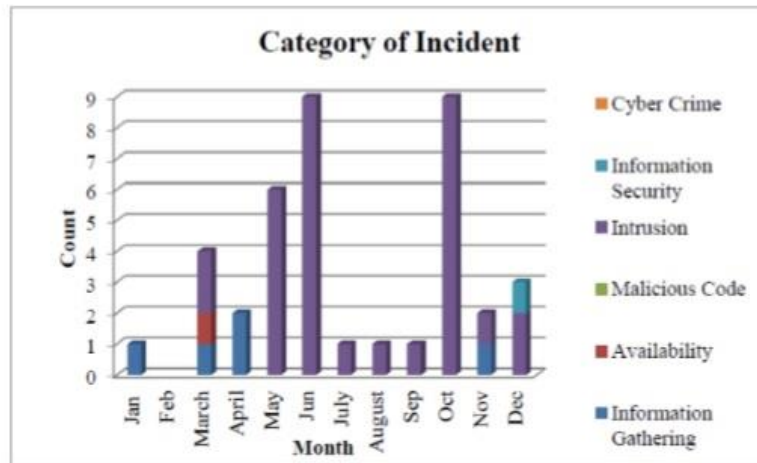
Cyber Crime Statistics 2016

Cyber Crime Cases in Myanmar 2017

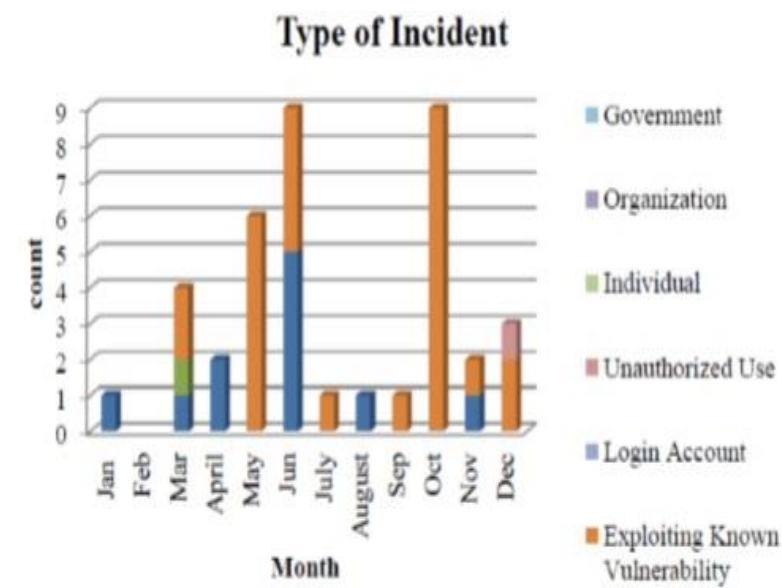


forensicsmyanmar

Cyber Crime Statistics 2017



MMcert 2018



MMcert 2018

Digital Forensics lab တည်ဆောက်ဖို့ နေရာ နဲ့ အဆောက်အဦးရွေးချယ်တော့မယ် ဆိုရင်အောက်ပါအချက်များကိုထည့်သွင်းစဉ်းစားရပါမယ်။

- Lab တစ်ခုလုံး Run နိုင်ဖို့ လျှပ်စစ်ဘယ်လောက်အတိုင်းအတာလိုအပ်သလဲ မီးပျက်သွားရင် ဘယ်လိုအစီစဉ်နဲ့ ဆက်ပြီး Runမလဲအဓိကဘယ်နေရာ တွေကို ဦးစားပေးအရ လျှပ်စစ် မပြတ်တောက်အောင်လုပ်မလဲ၊ အချိန် ဘယ်လောက်ကြာကြာ လျှပ်စစ်ပေးထားနိုင်မလဲ
- အထပ်မြင့်အဆောက်အဦးအတွက်ဆိုရင် ပစ္စည်းသယ်ယူဖို့လွယ်ကူခြင်း ရှိမရှိ။
- အဆောက်အဦးနဲ့ အခန်းနံရံနဲ့ အခန်းဖွဲ့စည်းပုံအရ ပြင်ပနှင့်အတွင်းဘက်မှ ဖောက်ထွင်းဝင်ရောက်ခြင်းမှကာကွယ်နိုင်ခြင်းရှိမရှိ
- အဆောက်အဦး၊နံရံ၊မျက်နှာကျက်၊ကြမ်းပြင်တွေက သဘာဝဘေးဒဏ်နဲ့ မီးဘေးမှ ကာကွယ်နိုင်ခြင်းရှိမရှိ၊
- အကြမ်းဖက်သမားများ၊သောင်းကျန်းသူများ၊ဒုစရိုက်သမားများ မှ ဝင်ရောက် ဖျက်ဆီး နိုင်မှုအနည်းဆုံးဖြစ်အောင်တည်ဆောက်စီမံခြင်း။
- ဆူပူအုံကြွမှု၊ ဆန္ဒပြမှုတို့ဖြစ်လာလျှင် Risk အနည်းဆုံးဖြစ်စေရန် စီမံခြင်း

Physical Security

CCTV Surveillance System

အဆောက်အဦး၊ အခန်းဖွဲ့စည်းပုံ၊ Lab တည်ဆောက်ပုံ အနေအထားအရ CCTV System ကို စနစ်တကျ တပ်ဆင်ထားရပါမယ်။ (eg- Three Foot Step)

Access control

ကိုယ်တတ်နိုင်တဲ့ budget အလိုက်၊ လုံခြုံရေးဦးစားပေးအလိုက် physical locks keys, electronic keypads, swipe cards, and/or biometrics စနစ်များ

Fire control System

မီးဘေးလုံခြုံရေးစနစ် မီးငြိမ်းသက်ရေးစနစ်များကို တပ်ဆင်ထားသင့်ပေမဲ့ ရေကြောင့် သက်သေခံအချက်အလက်များကို မပျက်စီးအောင် ကာကွယ်ထား ရပါမယ်။

Windows, doors & walls protection

အလွယ်တကူ ချိုးဖျက်ပြီး မဝင်ရောက်နိုင်စေရန် ပြုလုပ်ခြင်း၊ အရေးကြီးသော အခန်းများတွင် fireproof door များတပ်ဆင်ခြင်း၊ လုပ်ငန်းလုပ်ဆောင်ပုံနှင့် သက်သေခံ ပစ္စည်းများအား အပြင်မှ အလွယ်တကူမမြင်နိုင်စေရန် ပြုလုပ်ခြင်း

Radio jamming system

သက်သေခံပစ္စည်းများထားရှိသောအခန်းနှင့် လုံခြုံရေးအရ အရေးပါသော အခန်း နေရာများကို Bluetooth, Wireless Network, 2G 3G 4G Network, များမှနေပြီး နောက်ယှက်မှုမပြုနိုင်အောင် စီမံခြင်း။ Cooling System, Anti-static flooring များထားရှိခြင်း။

Off-site Data Storage Backup

အရေးကြီးသော အချက်အလက်များအား Lab မှာရှိတဲ့ Server ထဲတွင်သာမက အခြားသော Location များတွင်ပါ ထားရှိခြင်း။

Long Term Data Storage

သက်သေခံအချက်အလက်များကို သုတေသနပြုလုပ်ရန်အတွက်လည်းကောင်း၊ နောက်တစ်ချိန်တွင် မှီငြမ်းအသုံးပြုရန်အတွက်လည်းကောင်း ထားရှိခြင်း
(Long Term Data Storage အတွက် ထားရှိမည့်ကာလကို ဥပဒေတွင် ပြဋ္ဌာန်းသင့်သည်)

Digital Forensics lab အဆောက်အဦးအခန်းအကျယ်အဝန်းအလိုက် အခန်းဖွဲ့စည်းပုံ အငယ်ဆုံးအနေအထားကို ပုံမှာပြထားပါတယ်။ Lab သို့လာရောက်ပြီး Evidence အပ်နှံတဲ့နေရာ၊ Label ထပ်မံကပ်တဲ့နေရာ၊ Form ဖြည့်သွင်းတဲ့နေရာများကို တစ်နေရာထဲမှာ (သို့မဟုတ်) အကျယ်အဝန်းအလိုက် နှစ်နေရာ ခွဲနိုင်ပါတယ်။ သက်သေခံလာရောက်အပ်နှံသူက သက်ဆိုင်ရာ Examiner နဲ့အမှုအကြောင်း အသေးစိတ် ဆွေးနွေးလိုတယ်ဆိုရင် (အပ်နှံသူနှင့်ဆွေးနွေးသူကို) ထပ်မံ Register ပြုလုပ်ရပါမည်။

(မသမာမှုမပြုလုပ်နိုင်စေရန်)

Reception room ရဲ့နောက်ပိုင်းကိုတော့ Lab မှာတာဝန်ထမ်းဆောင်တဲ့ ဝန်ထမ်းသီးသန့်သာဝင်ရောက်ခွင့်ပြုရမှာဖြစ်ပါတယ်။ Imaging Room ကနေ Evidence Store Room ကိုသွားတဲ့လမ်းက အကွေ့အကောက်မရှိ ဝေးကွားမှုမရှိ ပဲ အတတ်နိုင်ဆုံး ကပ်ရပ် (သို့မဟုတ်) လမ်းကြောင်းတစ်ဖြောင့်တည်းရှိရပါမယ်။ (လက်နဲ့ကိုင် ဆောင်ပြီး ယူရချိန်နည်းအောင်နှင့်မသမာမှုမပြုလုပ်နိုင်ရန်ဖြစ်ပါသည်။) စစ်ဆေးတဲ့ အခန်းအလိုက် မှာ စစ်ဆေးသူများ သက်တောင့်သက်သာရှိစေရန် အခန်း အနေ အထား စားပွဲခုံ ထိုင်ခုံ စသည်တို့ကို စီစဉ်ဆောင်ရွက်ထားရပါမည်။ ရုံးပိုင်ဆိုင်ရာ စာရွက်စာတမ်း၊ Printer, Scanner စသည်တို့ထားရှိသော အခန်းကို lab မှာ ဝန်ထမ်းများ အဆင်ပြေစွာ အသုံးပြုနိုင်စေရန် အခန်းကို စီစဉ်ထားရပါမည်။ စစ်ဆေးသူများ Work Loading မဖြစ်စေရန် သီးသန့်နားနေရာများ၊ အခြားသော လိုအပ်ချက်များကိုစီမံထားရပါမည်။

ထပ်မံထည့်သွင်းစဉ်းစားရမည့်အချက်များ

- Reception ပြုလုပ်တဲ့နေရာနှင့် Lab နေရာကို ဝင်ရောက်တဲ့နေရာကို သိသန့်ထားရှိရမှာဖြစ်ပါတယ်။ (မလိုအပ်သော ဝင်ရောက်မှုများမဖြစ်စေရန်)
- Evidence Storage Room နဲ့ Server Room ကို သိသန့်ထားရှိရပါမည်။
- Evidence Storage Room နဲ့ Server Room ကို ဝင်ရောက်ရာတွင် သိသန့် Register လုပ်ပြီး ကန့်သတ်မှုများပြုလုပ်ထားရပါမည်။

- Imaging Room ကနေ Evidence Store Room

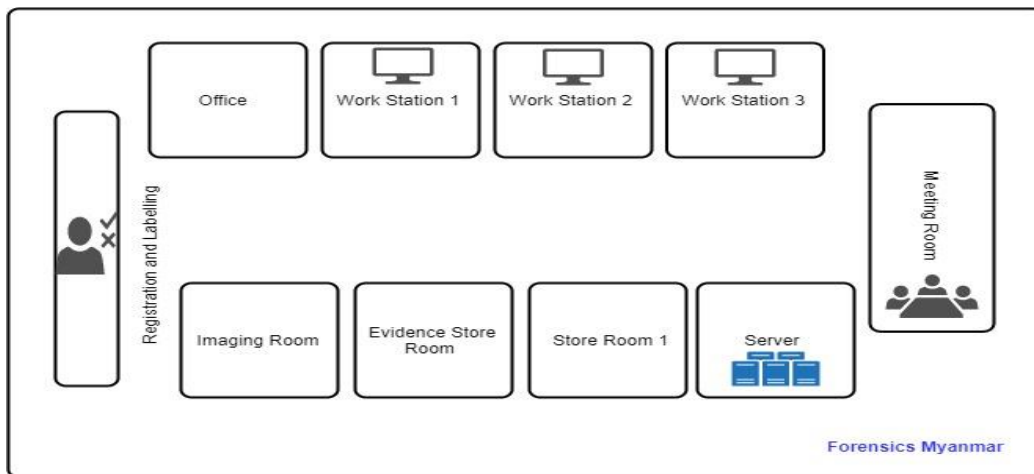
ဟာတတ်နိုင်သမျှနီးကပ်နေရပါမည်။

- လိုအပ်လာလျှင်ထပ်မံတိုးချဲ့မယ့် Work Station နေရာတွေထားရှိရပါမည်။

- Examiner များ သိသန့်အလုပ်လုပ်ရန် နေရာများသတ်မှတ်ပေးခြင်း

- Examiner အချင်းချင်းဆွေးနွေးမှုပြုလုပ်နိုင်ရန် နေရာများ (Projector/whiteboard တပ်ဆင်ပေးထားရပါမည်)

- Examiner များအတွက် သိသန့် Unlimited Internet Connection



Basic Digital Forensics Lab

Digital Forensics Lab ကိုလာရောက်တဲ့ ဝန်းထမ်းရဲ့ဧည့်သည်၊ အလုပ်သမား၊

အခြားသော ဌာနဆိုင်ရာမှလူများ၊ လာရောက်လေ့လာသူများ ကြောင့်

ပျက်စီးဆုံးရှုံးမှုမဖြစ်စေရန် သတင်းပေါက်ကြားမှုမဖြစ်စေရန်

- လာရောက်မည့်သူ၊ လာရောက်မည့်အရေအတွက် အကြောင်းအရာ အားကြိုတင်

အကြောင်းကြားစေခြင်း၊ registration Process အားစနစ်တကျပြုလုပ်ခြင်း၊

ရက်ကြာရှည်စွာလာရောက်သူများအတွက် temporary ID များထုတ်ပေးခြင်း၊

- လာရောက်သူများ မဝင်ရောက်စေရန် သတိပေးစာတမ်းများကပ်ထားခြင်း၊ ဓတ်ပုံ

ဗီဒီယိုရိုက်ကူးခြင်း များကို တားဆီးကန့်သတ်ခြင်း၊ လာရောက်သူများနောက်မှနေပြီး

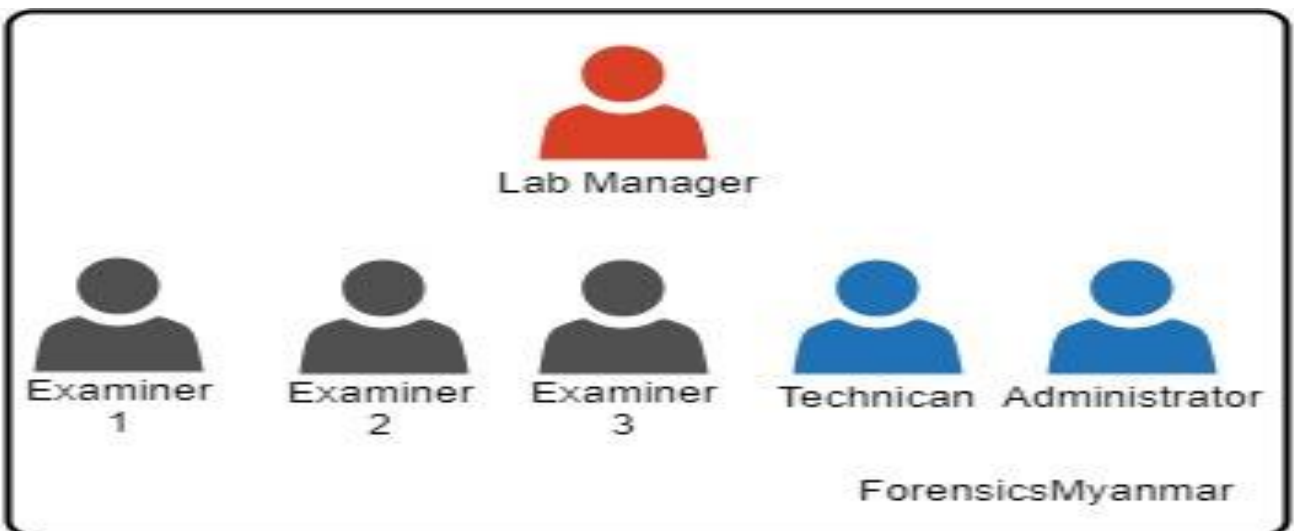
Lab မှတာဝန်ရှိသူများမှ စောင့်ကြည့်ခြင်း။

Digital Forensics Lab ပမာဏအလိုက် ဝန်ထမ်းများခန့်အပ်ရာတွင် အရေးအကြီးဆုံးအချက်မှာ ပညာအရည်အချင်းသာမက ဝန်ထမ်း၏ လက်ရှိအချိန်တွင်သာတင်မကပဲ ယခင်ကနောက်ကြောင်းရာဇဝင် ရှင်းလင်းမှုဖြစ်ပါသည်။အနိမ့်ဆုံးဝန်ထမ်းအဆင့်မှစတင်ပြီးနောက်ကြောင်းရာဇဝင်ရှင်းလင်းမှုကို အလေးထားဆောင်ရွက်ရပါမည်။

(အထူးသဖြင့် စစ်ဆေးသူ၏ Social Network အသုံးပြုမှု မှတ်တမ်းဖြစ်ပါသည်။ စစ်ဆေးသူသည် ပါတီနိုင်ငံရေးမကင်းရှင်း သော အရေးအသားများကို ရေးသားခြင်း အခြား မသင့်တော်သော အရေးအသားများရေးသားထားပါက တရားရုံးတွင် အဆိုပါ စစ်ဆေးသူ၏ အကြောင်းအရာ အချက်အလက်ကို တစ်ဖက်ရှေ့နေမှ ထောက်ပြကာ စစ်ဆေးမှုကို သံသယဝင်စေရန်ပြုလုပ်နိုင်ပါသည်။)

ပုံမှန်ပြထားတာက Lab တစ်ခု၏ အခြေခံအကျဆုံး Team ဖွဲ့စည်းမှုဖြစ်ပါသည်။ Lab ပမာဏအရ သက်ဆိုင်ရာ အပိုင်းအလိုက် Team များစွာရှိနိုင်ပြီး Team တစ်ခုတွင်လည်း လူများစွာပါဝင်နိုင်ပါသည်။

Team တစ်ခုတွင် အလုပ်လုပ်သောသူများကို သက်ဆိုင်ရာအပိုင်းလိုက် တာဝန်ကို တိကျစွာရှင်းလင်းပြော ဆိုထားရ မည်ဖြစ်ပါသည်။



Lab Manager

Lab Manager သည် သူတာဝန်ယူရသော အပိုင်းနှင့်ပတ်သက်သော နည်းပညာအကြောင်းအရာများကိုသိရှိထားရမည်ဖြစ်ပါသည်။ သက်ဆိုင်ရာအပိုင်းအလိုက် electronic (digital) evidence များကို စနစ်တကျ တရားဥပဒေလမ်းကြောင်းအတိုင်း တရားရုံးသို့တင်ပြနိုင်ရမည်ဖြစ်ပါသည်။ Digital Forensics lab တစ်ခုလုံးရဲ့ လုပ်ငန်းများအကြောင်းကိုလဲ နားလည်ထားရမည်ဖြစ်ပါသည်။ အသစ်ထွက်ရှိနေသောနည်းပညာများအကြောင်း၊ Forensics Hardware/Software များကိုလေ့လာစုံစမ်းဝယ်ယူခြင်း၊ ကိုယ်တာဝန်ယူရသော Lab အား install လုပ်ခြင်း၊ Update ပြုလုပ်ခြင်း၊ Team မှ ဝန်ထမ်းများကို ပြန်လည်သင်ကြားပေးခြင်း၊ လိုအပ်ပါက ကိုယ်တိုင်ပါဝင်လုပ်ဆောင်ခြင်း၊ သက်သေခံအချက်အလက်များကို နောက်ဆုံးအတည်ပြုပေးခြင်း၊ နည်းလမ်းမကျ သော အမှုများမှ သက်သေခံပစ္စည်းများကို ဥပဒေနည်းလမ်းအတိုင်း Reject ပြုလုပ်ခြင်းတို့ကို ပြုလုပ်ရမည်ဖြစ်ပါသည်။ (တရားနည်းလမ်းမကျသိမ်းယူသော သက်သေခံပစ္စည်းများ၊ First Responder Team မှ အဆင်အခြင်မဲ့စွာ လွှဲမှားစွာတရားနည်းလမ်းမကျ သိမ်းယူသော သက်သေခံပစ္စည်းများ)

Technician

Technician သည် အဓိကအားဖြင့် Imaging Room တွင်တာဝန်ယူရသောသူ၊ Evidence Storage Room တွင်တာဝန်ယူရသောသူ၊ Reception Room တွင်တာဝန်ယူရသောသူများဖြစ်ပါသည်။ Lab တစ်ခုချင်းစီ၏ Forensics Hardware/Software များကို update /maintain/repair/ ပြုလုပ်ရခြင်းများလဲ ပြုလုပ်ရပါသည်။ သက်ဆိုင်ရာအပိုင်းလိုက် နည်းပညာတင်သာမကပဲ၊ အခြားသောနည်း ပညာများကိုလဲ သိရှိထားရပါမည်။

Administrator

Administrator ကတော့ HR ပိုင်းတာဝန်၊ သက်ဆိုင်ရာ Team အလိုက် Lab အလိုက် စာရွက်စာတမ်းများကို စီစဉ်ပြုလုပ်သူဖြစ်ပါသည်။ liaison ပြုလုပ်ခြင်း၊ အခြားသော အဖွဲ့အစည်းများနှင့်ဆက်သွယ်ခြင်း Forensics Hardware/Software များကိုမှာယူခြင်းအပိုင်းတို့ကိုပြုလုပ်ရပါသည်။

Examiner

Examiner ကတော့ နည်းပညာဆိုင်ရာ အသိအမှတ်ပြုဘွဲ့တစ်ခု ရရှိထားရုံသာမကပဲ သက်ဆိုင်ရာကိုယ်စစ်ဆေးတဲ့ အပိုင်းလိုက်နည်းပညာ နှင့် ကိုယ်တွယ်အသုံးပြုသော Forensics Hardware/Software များရဲ့ Certificate များကိုရရှိထားရပါမည်။ တည်ဆဲဥပဒေများကို နားလည်ရုံသာမက အများနားလည်အောင် စစ်ဆေးပြီးစီးကြောင်း Report ကိုရေးသားနိုင်ရပါမည်။ စကားပြောဆိုမှုလိမ်မာပါးနပ်ပြီး ဆက်ဆံရေးကောင်းမွန်သူဖြစ်ရပါမည်။

သင်တန်းများပို့ချခြင်း/သင်တန်းစေလွှတ်ခြင်း

Lab တွင်တာဝန်ထမ်းဆောင်သောသူများကို တိုးတက်နေသော နည်းပညာများနှင့်မျက်ခြေမပျက်စေရန် သင်တန်းများပေးခြင်း၊ seminars များကို တက်ရောက်စေခြင်း၊အခြားနေရာများသို့သင်တန်းစေလွှတ်ခြင်းများကိုပြုလုပ်ရမည်ဖြစ်ပါသည်။ သင်တန်းစေလွှတ်ခြင်းဖြင့် နေရာသစ်ကိုရောက်သောကြောင့် စိတ်လန်းဆန်းစေရန်ဖြစ်ပါသည်။ မိမိကိုယ်တွင် အသုံးပြုသော Forensics Hardware/Software များရဲ့သင်တန်းများကိုလဲ

တက်ရောက်သင်ကြားရမည်ဖြစ်ပါသည်။ သို့မှသာ ယုံကြည်မှုရှိစွာကိုင်တွယ်နိုင်ပြီး
တရားရုံးတွင် အဆင်ပြေစွာ ထွက်ဆိုနိုင်မည်ဖြစ်ပါသည်။ အသစ်ရောက်လာသော
ဝန်ထမ်းများကိုလဲ သက်ဆိုင်ရာ အပိုင်းအလိုက် ဆရာတစ်ယောက်တွဲပေးခြင်း၊
နည်းပညာများကို လေ့လာရန်လွယ်ကူစေရန် အချင်းချင်း Share
လုပ်ပေးခြင်းများပြုလုပ်ရမည်ဖြစ်ပါသည်။
သင်တန်းတက်ရောက်သူများ လိုအပ်သော အဓိက အချက်မှာ
မိမိတက်ရောက်နေသောသင်တန်းမှာပို့ချသော သင်ခန်းစာသာများ
မိမိနှင့်အတန်းဖော်ထံမှလဲ ပညာရအောင်ယူနိုင်ရမည်ဖြစ်ပါသည်။
သင်တန်းများသို့စေလွှတ်ရာတွင် လည်း မိမိလက်အောက်မှ လူများ၏
အခြေအနေကိုကြည့်ပြီး အဆိုပါဝန်ထမ်းလိုအပ်လျှက်ရှိသော သင်တန်းများ၊ seminars
များကိုတက်ရောက်စေရမည်ဖြစ်ပါသည်။ သင်တန်းများ၊ဝန်ထမ်းများ၏
အခြေအနေကိုအမြဲမပြတ် Analysis များပြုလုပ်ရမည်ဖြစ်ပါသည်။ ဒါမှသာ Lab
အဆင့်အတန်းတိုးတက်ရုံသာမက ဝန်ထမ်းများနေပျော်ပြီး အလုပ်မြဲမှာဖြစ်ပါသည်။

Hardware/Software ဝယ်ယူမယ်ဆိုရင်ထည့်သွင်းစဉ်းစားရမဲ့ အချက်တွေကတော့
Lab မှာတစ်ကယ်တန်းအသုံးတည့်မတည့်၊ Software ဝယ်ယူတဲ့ ကုန်ကျငွေအပြင်
နှစ်စဉ်လိုင်စင်ဈေးနှုန်း၊သင်တန်းကြေး၊ Certificate ကုန်ကျငွေစတာတွေကို
ထည့်သွင်းတွက်ချက်ရမှာဖြစ်ပါတယ်။ အခြား Open Source တွေနဲ့အစားထိုး
အသုံးပြုရင် ဥပဒေ၊တရားရုံးမှာ အဆင်ပြေနိုင်မလား။ ဘယ်လို Case မျိုးဆို
အစားထိုးအသုံးပြုလို့ရနိုင်မလဲ။ မြန်မာနိုင်ငံမှာတော့ မလုပ်ခိုင်းသေးပေမဲ့
အခြားနိုင်ငံတွေမှာတော့ တရားရုံးကနေ လိုအပ်လာရင် အချို့သော Case တွေမှာ ‘dual
tool verification’ ကိုသုံးခိုင်း ပြခိုင်းပါတယ်။ ဘာလို့လဲဆိုရင် ပထမသုံးတဲ့ နည်းပညာ
နည်းလမ်းနဲ့ စစ်ဆေးတဲ့ သက်သေခံရလဒ်က နောက်ထပ်တူညီတဲ့
နည်းပညာနည်းလမ်းနဲ့ စစ်ဆေးတဲ့ သက်သေခံရလဒ် တူညီမှုရှိမရှိဆိုတာ
သေချာခြင်လို့ဖြစ်ပါတယ်။ (အရှင်းဆုံးဥပမာအနေနဲ့ဆိုရင် Hard Disk Data

Recovery လုပ်မယ်ဆိုရင် EaseUS နဲ့ခေါ်ရင် ဘယ်လိုရလဒ်ထွက်လဲ
နောက်တစ်မျိုး Recuva နဲ့လုပ်ရင် ဘယ်လိုရလဒ်ထွက်လာမလဲ
တူညီမှုရှိလား၊ကွဲပြားခြားနားလားဆိုတာ သိချင်လို့ဖြစ်ပါတယ်။

ဥပမာ Reception/Registration/Labeling လုပ်တဲ့နေရာမှာ အသုံးပြုတဲ့ Case Management Application။

Case Management Application မှာဘာတွေပါသင့်လဲဆိုရင်-

- Lab ကို သက်သေခံလာပို့တဲ့သူက ဘယ်သူ၊လာအပ်တဲ့ နေ့ရက်၊အချိန် လိပ်စာ အပြည့်အစုံ။ လက်ခံသူအမည်။
- သက်သေခံအချက်အလက် ပစ္စည်းစာရင်း။
- Case နံပါတ်၊ Case ရာဇဝင်၊ ဥပဒေပုဒ်မ။ (အရင် Case တွေနဲ့ပါ Analysis လုပ်နိုင်)။
- သက်သေခံပစ္စည်းကို စစ်ဆေးတဲ့သူအမည် (ပူးပေါင်းစစ်ဆေးသူများပါ အပါအဝင်) စတင်စစ်ဆေးချိန်၊ပြီးဆုံးချိန်သက်သေခံပစ္စည်းကို စစ်ဆေးတဲ့နည်းလမ်း အပြည့်အစုံ။
- စစ်ဆေးပြီးနောက် ရရှိလာတဲ့ သက်သေခံအချက်အလက်အပြည့်အစုံ။
- စစ်ဆေးသူနှင့်သက်သေခံလာရောက်အပ်နှံသူ တွေ့ဆုံမှု၊ဆက်သွယ်မှု အသေးစိတ်။
- သက်သေခံလာရောက်အပ်နှံသူထံလွှဲပြောင်းပေးအပ်တဲ့နေ့ရက်၊အချိန်၊တရားရုံးသို့ တင်ပြတဲ့နေ့ရက်အချိန်၊

(သက်ဆိုင်ရာအမှုစစ်တဲ့သူနဲ့ စစ်ဆေးသူကို မေးနိုင်သော မေးခွန်းများ (မမေးခဲ့ရင်တောင် သက်သေခံအချက်ပစ္စည်းက Lab ကိုရောက်တဲ့အချိန်ကစပြီး တရားရုံးကိုတင်ပြတဲ့အထိ စစ်မှန်ကြောင်းပြတဲ့အနေနဲ့ လိုအပ်လာရင် တင်ပြနိုင်ရမှာဖြစ်ပါတယ်)

What

သိမ်းဆည်းရမိတဲ့ Digital Device က ဘာလဲ ဘာကြောင့်သိမ်းတာလဲ

Where

Digital Device ကို ဘယ်နေရာကနေ သိမ်းတာလဲ သိမ်းဆည်းစဉ်မှာ
အခြေအနေကဘယ်လိုရှိလဲ
ဥပမာ။ power on or power off or damage .

How

အခင်းဖြစ်ရပ်မှာ လက်ရှိ ရှိနေတဲ့ Digital Device ကို စစ်ဆေးခဲ့လား
ဘယ်လိုစစ်ဆေးခဲ့လဲ ဘာတွေကို အသုံးပြုပြီး သက်သေစုဆောင်း
စစ်ဆေးခဲ့လဲ Integrity ရှိအောင် ဘာတွေလုပ်ခဲ့လဲ။ ဘာကို အသုံးပြုခဲ့သလဲ

How

သက်သေခံ Digital Evidences တွေကိုယ် ဘယ်လိုထုတ်ပိုးသလဲ။
ဘယ်လိုပို့ဆောင်လဲ။သယ်ယူပို့ဆောင်တဲ့ လမ်းကြောင်း။ ဘယ်လိုကိုင်တွယ်သလဲ။
ဥပမာ
(Mdy ကနေ YGN ကိုပို့တာ ၅ ရက်လောက်ကြာနေတာမျိုးမဖြစ်သင့်)

When

Digital Devices တွေ ဘယ်အချိန်မှာ Lab ကိုရောက်သလဲ
ဘယ်သူလက်ခံသလဲ။ဘာကြောင့်သူက လက်ခံရတာလဲ။

When

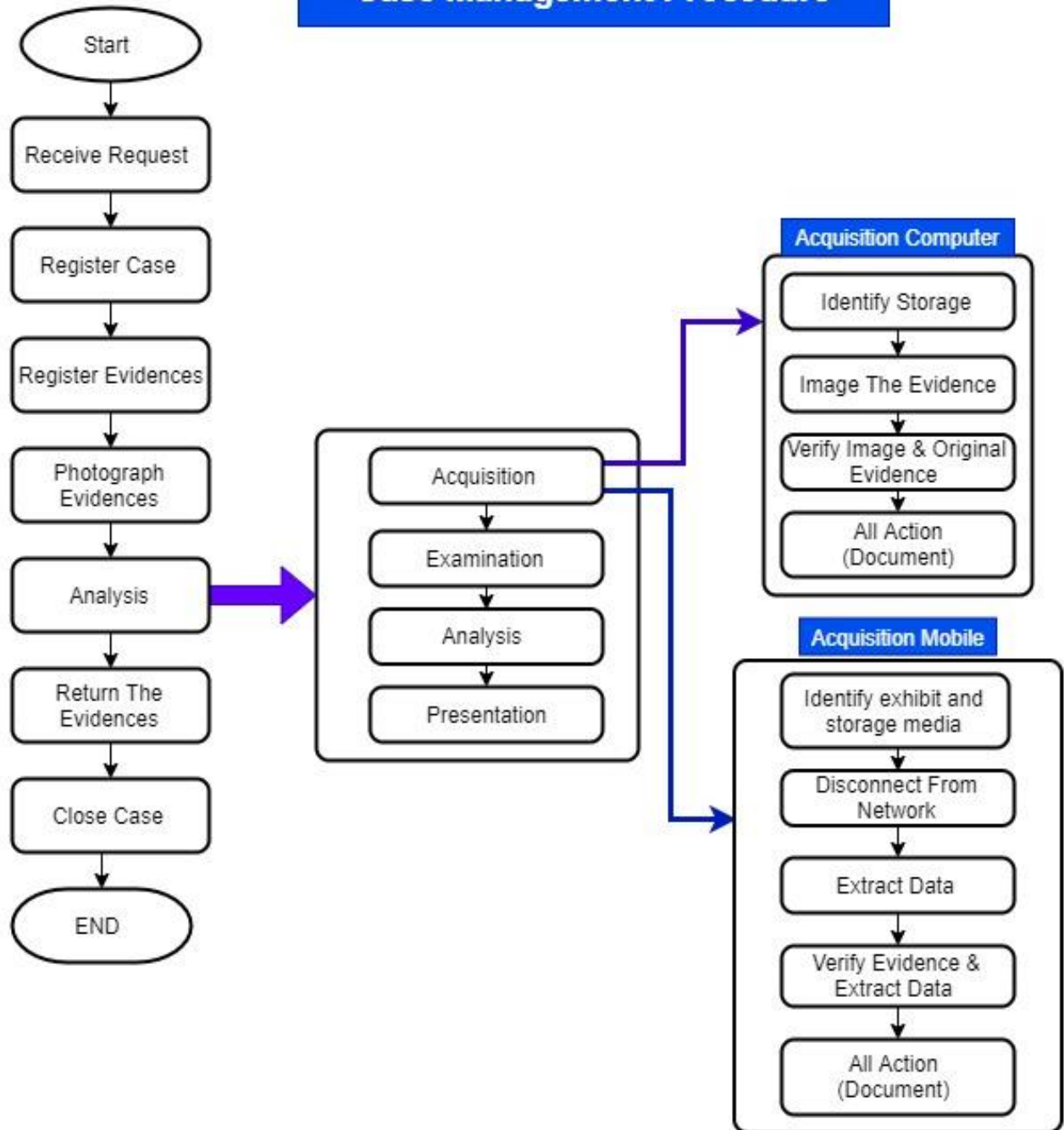
Digital Device ကိုဘယ်သူက ဘယ်အချိန်မှာ စတင်စစ်ဆေးတာလဲ။ စစ်ဆေးသူက
ဘာအကြောင်းကြောင့် ဒီ Digital Device ကို စစ်ဆေးရတာလဲ
ဘယ်သူတာဝန်ပေးတာလဲ။ဘယ်အချိန်မှာ စစ်ဆေးတာပြီးဆုံးလဲ။

How

Digital Device ကို ဘာ နည်းပညာ ကို အသုံးပြုပြီးစစ်ဆေးတာလဲ
အသုံးပြုသောနည်းလမ်းအမည် ။ စစ်ဆေးနေစဉ် သက်သေခံကို ကိုင်တွယ်ပုံ။

Case Management အပိုင်းနဲ့ ဆက်စပ်ပြီးဖတ်လိုက်ရင် နားလည်သွားမှာဖြစ်ပါတယ်။

Digital Forensics Lab Case Management Procedure



Case Management In Digital Forensics Lab

Receiving The Request

Lab ကိုစစ်ဆေးရန်အတွက် Request Letter ပို့မယ်ဆိုရင်တော့ E-government စနစ်ရှိနေရင် ကြိုတင်ပြီး သတ်မှတ်ထားတဲ့ Form ပုံစံရှိနေပြီး သားဖြစ် တဲ့အတွက် သတ်မှတ်ထားတာတွေဖြည့်ပြီးပို့လိုက်ရပါပဲ။ (ဒီနေရာမှာ ဖုန်းဖြင့်ပို့ လိုက်တဲ့ အချက်အလက်ကို ထပ်မံ အတည်ပြုဖို့တော့လိုအပ်ပါတယ်။ Form ထဲမှာဘာတွေ ပါဝင်လဲဆိုရင် အမှုရာဇဝင်၊ ဥပဒေပုဒ်မ၊ ပို့လိုက်တဲ့ သက်သေခံပစ္စည်း အသေးစိတ်အချက်အလက်၊ ထုတ်ပေးထားတဲ့ Warrant၊ စတင်သိမ်းဆည်းတဲ့ နေ့ရက် အချိန် အစရှိသည်ဖြင့်ပါဝင်ပါတယ်။ ပို့လိုက်တဲ့ Form ပုံစံက Reception/Registration /Labelling/ နေရာကိုရောက်လာတဲ့အခါ Lab Manager ဒါမှမဟုတ် အဲဒီနေရာမှာတာဝန်ကျနေတဲ့ Technical ဝန်ထမ်းက သတ်မှတ်ထားတဲ့စာရွက်စာတမ်းတွေ၊ အကြောင်းအရာအချက်အလက်တွေ ပြည့်စုံမှုရှိမရှိ စစ်ဆေးရပါတယ်။ Lab အနေနဲ့ထပ်ပြီး စဉ်းစားအတည်ပြုရမဲ့ အချက်တွေကတော့

- ရောက်ရှိလာတဲ့ သက်သေခံပစ္စည်းက lab နှင့်သက်ဆိုင်မှု ရှိမရှိ။
 - သိမ်းဆည်းလာစဉ်မှာ သက်သေခံပစ္စည်း အခြေအနေ။
 - Lab မှာစစ်ဆေးဖို့ နည်းပညာနဲ့နည်းလမ်းရှိမရှိ။
 - စစ်ဆေးပေးနိုင်မဲ့ ဝန်ထမ်းရှိမရှိ။
 - စာရွက်စာတမ်းပြည့်စုံမှု ရှိမရှိ။မသမာသောနည်းလမ်းနဲ့ ပြင်ဆင်ထားတာ ရှိမရှိ။
- အထက်ပါအချက်အလက်တွေပြည့်စုံမှုရှိလို့ Lab Manager မှလဲ အတည်ပြုရင် ပဏမအနေနဲ့ လက်ခံလို့ရပြီးဖြစ်ပါတယ်။

Registering The Case

သက်သေခံပစ္စည်း lab ကိုရောက်လာရင် တာဝန်ကျဝန်ထမ်းကနေ အမှုနဲ့ပတ်သတ်တဲ့ အချက်အလက်တွေကို Case Management Application (သို့မဟုတ်) သတ်မှတ်ထားတဲ့ Form ပုံစံစာရွက်ထဲမှာဖြည့်သွင်းလိုက်ပါတယ်။ အမှုအနေအထားအရ လာရောက်အပ်နှံသူနဲ့ Examiner က သက်သေခံပစ္စည်းထဲကနေ ဘယ်လိုအကြောင်းအရာ အချက်အလက်ကို ရယူခြင်တာလဲဆိုတာကို တိကျရှင်းလင်းစွာမေးမြန်းရပါတယ်။ ဒါမှသာ ဘယ်လိုအကြောင်းအရာ အချက်အလက်ကို ရှာဖွေရမယ်၊ ဘယ်လိုနည်းပညာ နည်းလမ်းသုံးရမယ်ဆိုတာကို စစ်ဆေးသူက ပြင်ဆင်နိုင်မှာဖြစ်ပါတယ်။ အပ်နှံသူနှင့် Examiner ဆွေးနွေးမှုမှတ်တမ်းကိုလဲ Case Management ထဲမှာ ထည့်သွင်းရပါတယ်။ (မသမာမှုမပြုလုပ်နိုင်စေရန်နှင့်အထောက်အထားရယူရန်) ဆွေးနွေးပြီးတဲ့အခါမှာ Lab ကနေ စစ်ဆေးရန်လက်ခံကြောင်းကို Lab မှ တာဝန်ရှိသူ (Reception Staff) ဒါမှမဟုတ် (Lab Manager, Examiner) နှင့် လာရောက်အပ်နှံသူ ကနေ လက်မှတ်ရေးထိုးရပါမည်။

Registering The Evidence Devices

Lab ကိုသက်သေခံပစ္စည်းရောက်တဲ့အချိန်မှာ အရေးအကြီးဆုံးဖြစ်တဲ့ သက်သေခံပစ္စည်းကို Sealed (စည်းတံဆိပ်ကပ်ထားခြင်း ရှိမရှိကို စစ်ဆေးရပါမည်။ စည်းမှာ ထုတ်ပိုးသူလက်မှတ်အတို၊ သယ်ယူတဲ့သူ၏ လက်မှတ်အတို၊ စည်းစကပ်တဲ့ရက်စွဲအချိန်တို့ပါဝင်ပါတယ်။)။ သက်သေခံ ပစ္စည်းကို သယ်ယူပို့ဆောင်တဲ့နေရာမှာ မသမာမှုမပြုလုပ်နိုင် စေရန်နှင့် သံသယကင်းစေရန်ဖြစ်ပါတယ်။ ။ Chanin Of Custody Form မှာလဲ သိမ်းဆည်းတဲ့နေ့ရက်အချိန်၊ Lab ကိုပို့ဆောင်တဲ့နေ့ရက် လာရောက်တဲ့

လမ်းကြောင်းခရီးပါဝင်ပါတယ်။ စည်းတံဆိပ်လဲမှန်ကန်တယ်
ဖျက်ရာပြင်ရာမရှိဘူးဆိုရင် စည်းကိုခွာပြီး သက်သေခံပစ္စည်း၊ ဆက်စပ် ပစ္စည်းတွေက
သိမ်းဆည်းစဉ်မှာရှိတဲ့အခြေအနေနဲ့တူညီမှုမရှိ၊မရှိ ပျက်စီးနေ မှုရှိ၊မရှိကို Case
Management ထဲမှာ တစ်ခုချင်း အသေးစိတ် ထည့်သွင်း ပါတယ်။
ဓာတ်ပုံမှတ်တမ်းပါသက်သေခံပစ္စည်းကို ရိုက်ယူထားပြီး Case Management ထဲမှာ
ထည့်သွင်းနိုင်ပါသည်။ (Negative Question ကို Lab
ဘက်မှကာကွယ်တဲ့အနေနဲ့အပြင်၊သက်သေခံပစ္စည်းမှန်ကန်စေရန်အတွက်ဖြစ်ပါသည်။)
အားလုံးမှန်ကန်ပြည့်စုံတဲ့အခါ Chain Of Custody Form မှာ Lab ကနေ
သက်သေခံပစ္စည်းကိုလက်ခံကြောင်း အပ်နှံသူနှင့်လက်ခံသူက လက်မှတ်ရေး
ထိုးရပါမည်။လတ်တလော မစစ်ဆေးနိုင်သေးတဲ့ သက်သေခံပစ္စည်းဆိုရင် Evidence
Store Room ထဲမှာထည့်သွင်း ထားရမှာဖြစ်ပါတယ်။

Photograph The Evidence Devices

သက်သေခံပစ္စည်းကို ဓာတ်ပုံရိုက်ယူရတာကတော့ ပစ္စည်းအခြေအနေ (example Ph
ဆိုရင် Power On နေလား Off နေလား) ပျက်စီးနေမှု စတာတွေကို
အရပ်မျက်နှာပေါင်းစုံကနေ ရိုက်ယူထားပြီး Negative Questions မမေးနိုင်စေရန်
မှန်ကန်မှုရှိစေရန်ဖြစ်ပါတယ်။ စစ်ဆေးပြီးတဲ့အခါ သက်ဆိုင်ရာကို
ပြန်လည်အပ်နှံတဲ့နေရာမှာလဲ အထောက်အထား ခိုင်လုံစေရန်ဖြစ်ပါတယ်။

Analysis

သက်သေခံပစ္စည်းကို Examiner ကနေ အမှုအနေအထား ရယူလိုတဲ့
သက်သေခံအကြောင်းအရာအချက်အလက်အပေါ်မူတည်ပြီးစစ်ဆေးတာဖြစ်ပါတယ်။

စစ်ဆေးတဲ့နည်းလမ်း အသုံးပြုတဲ့နည်းပညာ စတင်စစ်ဆေးချိန်
စစ်ဆေးမှုပြီးစီးသည့်အချိန်၊ စစ်ဆေးစဉ်ကာလမှာ အမှုအနေအထားအရ
သက်ဆိုင်ရာနှင့်ဆက်သွယ်မှု စတဲ့မှတ်တမ်းတွေကို Case Management
ထဲမှာထည့်သွင်းရမှာဖြစ်ပါတယ်။

Return The Evidences

စစ်ဆေးမှုပြီးဆုံးတဲ့အခါမှာ ရရှိလာတဲ့ Report နှင့် သက်သေခံပစ္စည်းကို သက်ဆိုင်ရာ
ဒါမှမဟုတ် လာရောက်အပ်နှံသူထံလွှဲပြောင်းပေးတာဖြစ်ပါတယ်။ လာရောက်အပ်နှံစဉ်က
ပစ္စည်းအခြေအနေ၊ ယခုပြန်လည်လွှဲပြောင်းတဲ့ ပစ္စည်းအခြေအနေကို
လာရောက်ယူတဲ့သူကို ရှင်းလင်းပြသပြီး lab ကနေ နောက်တစ်ခါ
သက်သေခံပစ္စည်းပေါ်ကို စည်းကမ်းပေးလိုက်ပါတယ်။

Closing The Case

စစ်ဆေးတဲ့အမှုလုံးဝ ပြီးသွားတဲ့အချိန်၊ အမှုပိတ်ကြောင်းကိုလဲ
နှစ်ဖက်လုံးသဘောတူတဲ့အချိန်မှာ အမှုပြီးစီးကြောင်း ကို သက်သေခံပစ္စည်း
လာရောက်အပ်နှံသူဘက်နေ လက်မှတ်ထိုးပြီး Lab ကိုပေးရမှာဖြစ်ပါတယ်။ ဒါမှသာ
Lab ဘက်ကနေ Examiner ထံမှာကျန်ရှိနေတဲ့ သက်သေခံအချက်အလက်တွေကို
ဆက်လက်သိမ်းဆည်းထားသင့်၊ မသင့် အပြီးတိုင် ဖျက်ဆီးရန် ဒါမှမဟုတ် Research
and Analysis ဥပဒေအရ ဘယ်ကာလအထိ ထိမ်းသိမ်းထားမယ်ဆိုတဲ့အပေါ်မူတည်ပြီး
လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။

Acquisition (Data Acquisition)(Forensically Sound) (Bits By Bits Copy) (Forensics Image)

Forensics Image ကိုဘယ်အချိန်မှာပြုလုပ်လဲဆိုရင် Lab ရဲ့ Reception, Registration/label အခန်းကနေမှတ်ပုံတင်ပြီးတာနဲ့ Case အခြေအနေအရ Image လုပ်တဲ့ အခန်းမှာသီးသန့်ပြုလုပ်တာဖြစ်ပါတယ်။ Evidence Store Room ထဲမှာ သိမ်းထားပြီးနောက်ပိုင်း စစ်ဆေးမှုပြုလုပ်ရမဲ့အခါမှာလဲ Image လုပ်တဲ့ အခန်းမှာပြုလုပ်ရမှာဖြစ်ပါတယ်။ Forensics Image လုပ်တဲ့ Storage Media ကိုမပြုလုပ်ခင်မှာ Lab မှာအသုံးပြုတဲ့ Wipe လုပ်တဲ့ Hardware ထဲမှာထည့်သွင်းပြီး Wipe ပြုလုပ်ထားရမှာဖြစ်ပါတယ်။ (အရင်ကအချက်အလက်တွေကို မပါလာစေချင်တဲ့အတွက်ဖြစ်ပါတယ်။

Acquisition ဆိုတာက စစ်ဆေးရမယ့် Digital Device (Hard disk, SSD, Memory Card, Flash Drive,Etc..) တို့ထဲမှာရှိတဲ့ အချက်အလက်တွေကို မူရင်းအတိုင်း ပြောင်းလဲပြင်ဆင်ခြင်းမပြုပဲကူးခြင်းဖြစ်ပါတယ်။ Analysis လုပ်တဲ့အခါမှာ မူရင်းသက်သေခံပစ္စည်းကိုစစ်ဆေးခြင်းမပြုပဲ သက်သေအဖြစ် သာသိမ်းဆည်းထားပါတယ်။ မူရင်းပစ္စည်းကနေကူးယူထားတဲ့ Forensics Image ကိုပဲစစ်ဆေးရတာဖြစ်ပါတယ်။ Forensics Image ပြုလုပ်ပြီးတဲ့အခါ မူရင်းသက်သေခံပစ္စည်းမှ Hash Value နဲ့ Forensics Image က Hash Value ကို မဖြစ်မနေ Record လုပ်ထားပါတယ်။(မူရင်းနဲ့ Forensics Image က အတူတူပဲဖြစ်ကြောင်း ပြနိုင်ဖို့အတွက်ဖြစ်ပါတယ်။) မူရင်းနဲ့ Forensics Image က Hash Value က တန်ဖိုးအတူတူပဲဖြစ်ရပါမယ်။ အသုံးပြုတဲ့ Hash Value ကတော့ MD5,SHA256, Etc ...။ အသုံးပြုတဲ့ Forensics Software/Hardware မှာ Hash ကို Generate လုပ်ဖို့ပါထားပြီးဖြစ်ပါတယ်။ စစ်ဆေးဖို့အတွက်ပြုလုပ်ထားတဲ့ Forensics Image က မူရင်းသက်သေခံပစ္စည်းထဲမှာ သိမ်းထားခြင်းမပြုရပါဘူး။ သီးသန့် Storage Device ပေါ်မှာပြုလုပ်ရခြင်းဖြစ်ပါတယ်။ Forensics Image ပြုလုပ်ထားတဲ့ Storage Device ကိုလဲ မူရင်းပစ္စည်းနဲ့ကွဲပြားအောင် Label သတ်မှတ်ပေးထားရပါမယ်။ Forensics Image လုပ်တဲ့ Process ကိုလဲ Case Management ထဲမှာ ထည့်သွင်းမှတ်တမ်းတင်ရမှာဖြစ်ပါတယ်။ Forensics Image ပြုလုပ်တဲ့ ရက်စွဲအချိန်၊ပြုလုပ်တဲ့သူ၊အသုံးပြုတဲ့ နည်းလမ်း၊ မူရင်းနဲ့ Forensics Image မှ Hash Value တူညီမှု၊ အသုံးပြုတဲ့ Hash Value MD5 Or SHA။

Acquisition ပြုလုပ်တဲ့အခါမှာ Case ပေါ်မူတည်ပြီး နှစ်မျိုးပြုလုပ်ပါတယ်။ Physical data acquisition နဲ့ logical data acquisition တို့ဖြစ်ပါတယ်။ ဒါပေမဲ့ တော်တော်များများကတော့ Physical data acquisition (The Whole Disk) ပဲပြုလုပ်တာများပါတယ်။ တစ်ကယ်လို့ System က Power On နေမယ်ဆိုရင် Live Acquisition ပါပြုလုပ်ပါတယ်။ Acquisition လုပ်မယ်ဆိုရင် မူရင်းပစ္စည်းနဲ့ တစ်ဆင့်ပြန်ကူးယူမဲ့ Device ကြားမှာ write blocker ထားရှိပါတယ်။ မူရင်းပစ္စည်းမှာရော Forensics Image မှာပါ Only Readable ပဲဖြစ်အောင်ဖြစ်ပါတယ်။ Acquisition လုပ်တဲ့အခါမှာ အချက်အလက်တွေကိုပြင်ဆင်ပြီး ကူးယူတာမဟုတ်ကြောင်း Negative Question မေးနိုင်အောင်ဖြစ်ပါတယ်။ Forensics Image လုပ်တဲ့ Tools တိုင်းမှာ Write Blocker ပါဝင်တာများပါတယ်။ Imaging Tools တွေဝယ်ယူမယ်ဆိုရင် Transfer Speed များတဲ့ဟာကိုအပဲ အဓိကထားပြီးဝယ်ယူကြပါတယ်။ Forensics Image File Type တွေကတော့ အသုံးပြုတဲ့ နည်းလမ်းနှင့် Case အပေါ်မူတည်ပြီး အမျိုးမျိုးရှိပါတယ်။

Acquisition On Computer

Identify Storage Media

Computer ရဲ့ Storage ပမာဏကိုစစ်ဆေးပြီး Forensics Image ပြုလုပ်ဖို့အတွက် Second Storage ကိုရွေးချယ်ပါတယ်။ Size ပမာဏ အရမ်းများနေရင် NAS Or Server ပေါ်ကိုဆွဲတင်ပါတယ်။

Imaging the Evidence နှင့် Verify Original Evidence and Image File

မူရင်းသက်သေခံပစ္စည်းကို Write Blocker နဲ့ချိတ်ဆက်ပြီး Hash Value ထုတ်ပါတယ်။ Evidence ကို Bits By Bits Copy ကူးယူပြီးတာနဲ့ Second Image ရဲ့ Hash Value ထုတ်ပါတယ်။ Hash Value 2 ခုလုံးတူညီရမှာဖြစ်ပါတယ်။

Document The All Action

Image လုပ်တဲ့ Process တိုင်းကို Case Management ထဲမှာ ဒါမှဟုတ် Document ပြုလုပ်ပါတယ်။

Data Extraction Mobile Devices

Identify the Exhibit and Storage Media

မစစ်ဆေးခင်မှာ Mobile Phone ရဲ့ Model, Mobile Equipment Identity Number (IMEI), a Mobile Equipment Identifier (MEID) or Serial Number တွေကို Label ပြုလုပ်ရပါတယ်။ Case အရ Cell Site Analysis ပြုလုပ်ဖို့လိုအပ်လာရင် လွယ်ကူအောင်ဖြစ်ပါတယ်။ ဖုန်းမှာပါလာတဲ့ SIM card Memory Card တွေကိုတော့ သီးသန့် Forensics Image ပြုလုပ်ပါတယ်။ နောက်ပြီးရင် Mobile Phone ရဲ့ Internal Storage ပမာဏကို စစ်ဆေးပါတယ်။

Disconnect From Any Network

ပြင်ပ Signal နှောက်ယှက်မှုမရှိတဲ့အခန်းထဲမှာပြုလုပ်ရတာဖြစ်ပါတယ်။ Jamming System မရှိရင်လဲ Airplane mode ပြုလုပ်ပြီး Wireless , Bluetooth, NFC ကိုပိတ်ထားရင် အဆင်ပြေပါတယ်။

Extract Data

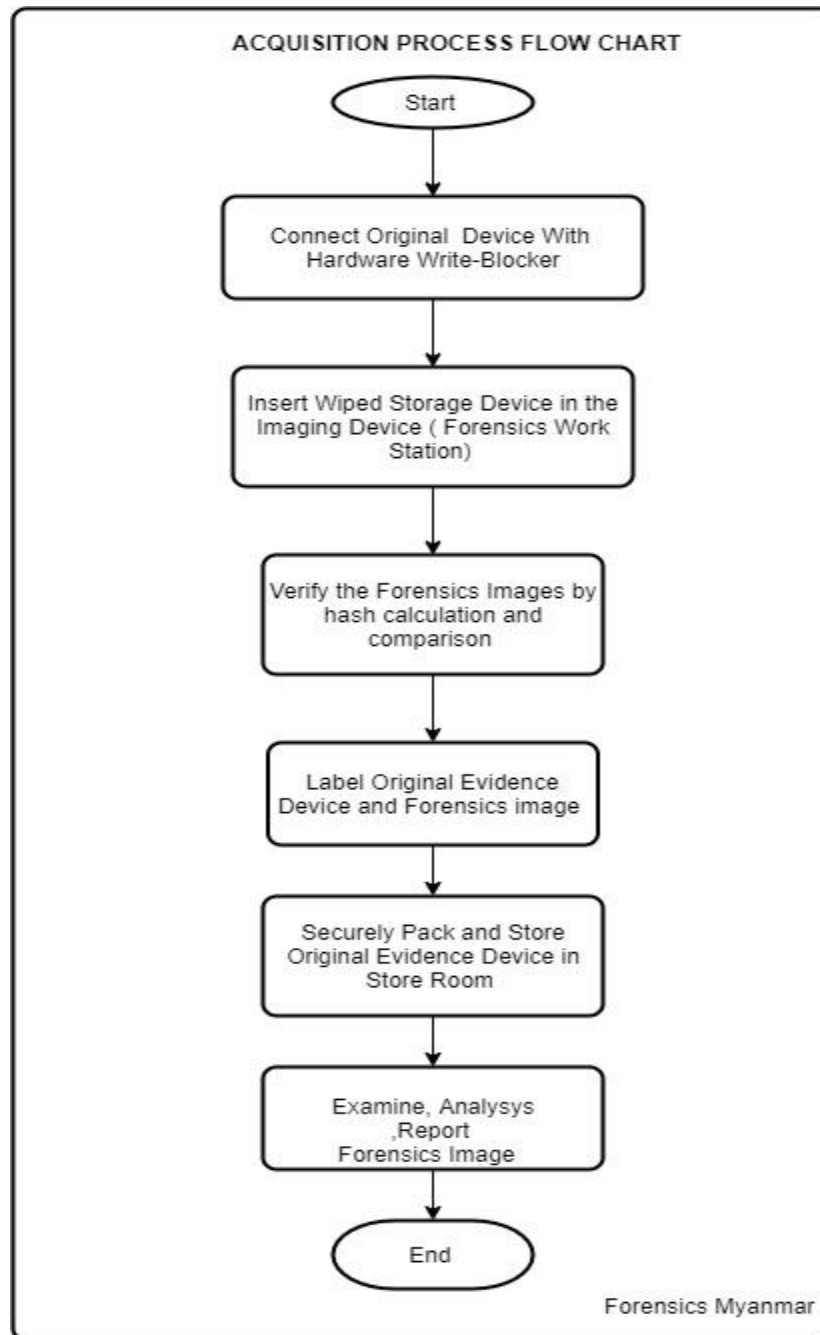
Case အနေအထားအရ Mobile phone ထဲကနေ အချက်အလက်များကိုရယူတာဖြစ်ပါတယ်။ ဖုန်းအမျိုးအစားအလိုက် Operation System အလိုက်မျိုးစုံကွဲပြားပါတယ်။ အသုံးပြုရတဲ့နည်းလမ်းလဲ အမျိုးမျိုးရှိပါတယ်။

Verify The Evidence and Extract Data

Mobile phone ကနေရယူထားတဲ့ အချက်အလက်ဟာ မူရင်းအချက်အလက်နဲ့တူညီမှုရှိမရှိ စစ်ဆေးခြင်းဖြစ်ပါတယ်။ (write Protect ပြုလုပ်တာက Mobile Phone Forensics မှာမပါဝင်ပါဘူး)

Document The All Action

ပြုလုပ်တဲ့ Process တိုင်းကို Case Management ထဲမှာ ဒါမှဟုတ် Document
ပြုလုပ်ခြင်းဖြစ်ပါတယ်။



Examination နဲ့ Analysis အကြောင်းက

အရင်ကရေးထားတာတွေထဲမှာစစ်ဆေးပုံစစ်ဆေးနည်းရော
တွေးပုံတွေးနည်းတွေကိုရေးထားပါတယ်။ ထက်မရေးတော့ပဲ အရေးကြီးတဲ့
အပိုင်းတွေသာ ဖော်ပြသွားပါမယ်။ အရေးကြီးတာက စစ်ဆေးတဲ့အခါ Forensics
Image နဲ့ပုံစစ်ဆေးရမှာဖြစ်ပါတယ်။ မူရင်း Evidence ကို
မပျက်စီးစေလိုတဲ့အတွက်ရော၊ စစ်ဆေးစဉ်အမှားဖြစ်သွားခဲ့ရင် မူရင်း Evidence
ပျောက်ကွယ်သွားမှာစိုးတဲ့အတွက်ဖြစ်ပါတယ်။ နောက်တစ်ခုက Mobile Forensics မှာ
Data Extract လုပ်တဲ့အခါ Write Protect သုံးလို့မရပါဘူး။ Boot loader ကနေ
Mobile phone ရဲ့ Internal Memory ကိုဆွဲယူလို့မရတဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။
အဲဒီအစား စစ်ဆေးသူရဲ့ Detail Process ကို Case Management ဒါမှမဟုတ်
Document မှာမှတ်တမ်းတင်ရမှာဖြစ်ပါတယ်။

Triage Method ကိုတော့ Lab မှာလဲအသုံးပြုပါတယ်။ အရေးကြီးရဲ့သာမက
အလျင်အမြန်စေဆေးပေးရမယ့် Case တွေမှာဖြစ်ပါတယ်။ ဥပမာ (အကြမ်းဖက်မှု)။
တိုးတက်နေတဲ့နိုင်ငံတော်တော်များများကတော့ Case ဖြစ်တဲ့နေရာမှာတင်ပဲ Expert
First Responder Team အဖွဲ့နဲ့ Result ရယူပါတယ်။ Triage Method ကို
ဘယ်အချိန်မှာအသုံးပြုလဲဆိုတော့ စစ်ဆေးရမဲ့ Device တွေအများကြီးရှိတဲ့အချိန်၊
အဖြေကိုချက်ခြင်းထုတ်ပေးရမယ့်အချိန်၊ Evidence Device ကို အချိန်အကြာကြီး
ထိမ်းသိန်းထားလို့မရနိုင်တဲ့အခြေအနေတွေမှာ အသုံးပြုပါတယ်။
အထက်ပါအခြေအနေတွေကြောင့် Triage Method အသုံးပြုမယ်ဆိုရင် လျင်မြန်ပေမဲ့
သက်သေခံအချက်အလက်အပြည့်အစုံရရှိနိုင်မှာမဟုတ်ပါ။ ခြွင်းချက်အနေနဲ့ Case အရ
တရားရုံးမှာ Triage Method ကိုအသုံးပြုထားကြောင်းတရားဝင်
တင်ပြထားရမှာဖြစ်ပါတယ်။ စစ်ဆေးသူအနေနဲ့လဲ Triage Method
အသုံးပြုပြီးဆိုတာနဲ့ အဖြေကိုအလျင်အမြန်ထုတ်ပေးရမှာဖြစ်ပြီး၊ Evidence
မပြည့်စုံမှာဖြစ်တာကြောင့် လက်ရှိထုတ်ပေးရမည့်အဖြေအပြင် နောက်တစ်ဆင့်မှာ
ဘာတွေဆက်စစ်မယ်၊ဘာလုပ်မယ်ဆိုတာကို Report
ထဲမှာထည့်ရေးပေးလိုက်ရမှာဖြစ်ပါတယ်။ Triage အတွက်စဉ်းစားလုပ်ဆောင်ရမည့်
Flow ကို Diagram နဲ့ဖော်ပြထားပြီးပါပြီ။

Digital Forensics လုပ်ဆောင်တဲ့အခါ Visualization Methods အများအပြားမှာ
ရှင်းလင်းအောင်၊စစ်ဆေးသူကိုယ်တိုင်လဲ ရှင်းလင်းစွာဖော်ထုတ်နိုင်ရန်အသုံးပြုပါတယ်။

Timeline ဖြင့် User တစ်ယောက်လုပ်ဆောင်တဲ့ အရာမှန်သမျှကို
ဖော်ပြခြင်း။ Relationship Diagram (Communication diagram)
ဖြင့် လူတစ်ယောက်နဲ့တစ်ယောက်ဆက်နွှယ်မှုကိုဖော်ပြခြင်း၊
Money Flow Diagram ဖြင့် ငွေကြေးဆက်နွှယ်မှု၊
ငွေကြေးစီးဆင်းမှုများကိုဖော်ပြခြင်း။

Electronic Evidence (Digital Evidence) မှာပြည့်စုံမည့်ယေဘုယျအချက်များမှာ
မူရင်းသက်သေခံ Device နဲ့ Forensics Image
သည်ကွဲလွဲမချက်မရှိရပါ။ သက်သေခံအချက်အလက်ကို Report ရေးရမှာ
တစ်ဖက်သတ်လိုရာဆွဲပြီးရေးသားခြင်းမပြုလုပ်ရပါ။ Lab ကို Evidence Device
ရောက်လာတဲ့အချိန်ကနေစပြီး Evidence Device
ကိုကိုင်တွယ်ခြင်း၊ စစ်ဆေးခြင်းအပိုင်းများတွင် သံသယဝင်ဖွယ်
အချက်အလက်များမရှိရပါ။ တရားရုံးကိုတင်ပြသော
သက်သေခံအချက်အလက်များသည် အများယုံကြည်လက်ခံနိုင်ရမည်ဖြစ်ပါသည်။
သက်သေခံကိုစစ်ဆေးသောနည်းလမ်းများသည် တစ်ဖက်စွန်းမရောက်စေပဲ
မျှတမှုရှိရမည်ဖြစ်ပါသည်။ Report ရေးသားရာတွင်လည်း အများနားလည်စေနိုင်မည့်
စကားလုံးအသုံးအနှုန်းများကိုသုံးစွဲဖော်ပြရမည်ဖြစ်ပါသည်။ Digital Forensics သည်
အခြာသောမူရင်းစစ်ဆေးနည်းများနှင့်ကွဲပြားတာကြောင့်
သက်သေခံသိမ်းဆည်းသည့်အပိုင်း၊ ကိုယ်တွယ်သည့်အပိုင်း၊
သယ်ယူပို့ဆောင်သည့်အပိုင်း၊ စစ်ဆေးသည့်အပိုင်းများတွင်
ဂရုတစိုက်ပြုလုပ်ဆောင်ရွက်ရမည်ဖြစ်ပါသည်။

Digital Forensics Lab QOS

သက်သေခံအချက်အလက်များကို တရားရုံးကိုတင်ပြတဲ့အခါ (အချို့သော Case
များတွင် Expert Witness မလိုအပ်ပါ။ အချို့သော အမှုများတွင်လိုအပ်ပါသည်။)
စစ်ဆေးသောသူသည် သက်သေခံအချက်အလက်ထင်မြင်ယူဆချက်သာမက
စစ်ဆေးသောနည်းလမ်း၊ အသုံးပြုသော Software/Hardware၊
စစ်ဆေးတဲ့အချိန်အစမှပြီးဆုံးတဲ့အချိန်အထိ လုပ်ဆောင်သမျှလုပ်ဆောင်ချက်များကို
တရားရုံးတွင် တင်ပြရပါသည်။ ထိုသို့တင်ပြနိုင်အောင် Digital Forensics Lab သည်
အောက်တွင်ဖော်ပြထားတဲ့အချက်များနှင့်ပြည့်စုံနေရမည်ဖြစ်ပါသည်။

Digital Forensics Lab အနေဖြင့် Lab တစ်ခုလုံးအလိုက်
သက်ဆိုင်ရာအပိုင်းအလိုက်ဖွဲ့စည်းထားရှိမှုဇယားလုပ်ဆောင်ထားခြင်း
လစဉ်နှစ်စဉ် lab ရှိ လုပ်ငန်းစဉ်များ၊စာရွက်စာတမ်းသိမ်းဆည်းပုံ၊စက်ပစ္စည်းများအား
စစ်ဆေးခြင်း

Negative Question များတွက် ပြန်လည်သုံးသပ်ခြင်း၊ပြင်ဆင်ခြင်း၊

Lab အား External,Internal Access Permission များအားစောင့်ကြည့်စစ်ဆေးခြင်း၊
အဆင့်မြှင့်တင်ခြင်း။

Lab နှင့်သက်ဆိုင်သော ပစ္စည်းများ (Hardware/Software) အားအဆင့်မြှင့်တင်ခြင်း၊
ပြန်လည်ပြင်ဆင်ခြင်း

မစစ်ဆေးခင်မှာ Lab ပစ္စည်းများ ပုံမှန်လုပ်ဆောင်မှုရှိ၊မရှိ စစ်ဆေးခြင်း

(အလုပ်မဝင်ခင်အချိန်၊အလုပ်လုပ်နေစဉ်အချိန်များတွင်) Lab မှဝန်ထမ်းများ၏

Personal Security အားစောင့်ကြည့်စစ်ဆေးခြင်း။

Lab အတွင်းသင်တန်းများပို့ချခြင်း၊

သက်ဆိုင်သောအပိုင်း၊အားနည်းသောအပိုင်း၊လိုအပ်သောအပိုင်းများအတွက်

သင်တန်းများစေလွှတ်ခြင်း။

ဝန်ထမ်းအသစ်များအား သင်တန်းများပေးခြင်း။

တည်ဆဲဥပဒေများနားလည်စေရန် သင်တန်းများပေးခြင်း။ Workshop/Seminar
များပေးခြင်း။

သက်ဆိုင်ရာအပိုင်းအလိုက် စစ်ဆေးပုံနည်းလမ်းများအား Document များပြုလုပ်ခြင်း။

Forensics Software/hardware အလိုက် စစ်ဆေးပုံနည်းလမ်းများအား Document
များပြုလုပ်ခြင်း။

အခြားသော Lab များနှင့်ဆက်သွယ်ပေါင်းစပ်လုပ်ကိုင်ခြင်း၊ နည်းပညာအသစ်များ

နည်းလမ်းများကို စဉ်ဆက်မပြတ်လေ့လာခြင်း။

နိုင်ငံတစ်ကာနှင့်ဆက်စပ်သော Case များတွင် နိုင်ငံတစ်ကာမှ လက်ခံလာနိုင်အောင်

International Law နှင့်အညီစစ်ဆေးခြင်း။

ဥပဒေအရ လက်ခံစစ်ဆေးရမည့်အကြောင်းအရာ၊

လက်မခံရမည့်အကြောင်းပြချက်များကိုသတ်မှတ်ခြင်း။

Evidence ကိုင်တွယ်ခြင်းနှင့်ပတ်သတ်ပြီး လုံခြုံစွာသယ်ယူပို့ဆောင်မှု၊သတ်မှတ်ထားည့်

စာရွက်စာတမ်းများ စည်းတံဆိပ်များပါဝင်ခြင်း ရှိ၊မရှိ။

သက်သေခံပစ္စည်းထားရှိသည့်အခန်း ထားသို့မူထုတ်ပေးမှု၊လက်ခံမှု၊စနစ်ကျမှုရရှိ၊မရှိ။
လုံခြုံမှုရှိ၊မရှိ။

ပြီးစီးပြီး Case များမှ Report များကို စနစ်တက်ထားရှိရှိ၊မရှိ။

စစ်ဆေးပြီး Evidence Device များ ပြန်လည်လွှဲပြောင်းရာတွင် စနစ်တကျရှိ၊မရှိ။

Forensics Report များသတ်မှတ်ထားသော အဆင့်အတန်းနှင့် ညီ၊မညီ။

Digital Forensics Lab အတွင်းရှိ လှုပ်ရှားဆောင်ရွက်မှုများလုံခြုံစိတ်ချစွာ

စောင့်ကြည့်မှု၊ မှန်ကန်မှုပေးနိုင်ရန် ISO 17025

စနစ်များနှင့်ဆက်စပ်ပြီးလုပ်ဆောင်ရမည်ဖြစ်ပါသည်။